Privacy- en Securitybeleid

Team P&S

8-3-2024 | Versie 1.1

Vervangingsfonds
Participatiefonds

Versiebeheer

Versie	Datum	Wijziging	Auteur(s)
1.0	14 januari 2021	Vaststelling definitieve versie	I. Coppens en M. Wieërs (Privacy & security officer)
1.1 concept	30-1 t/m 22-2 2024	Periodieke review i.s.m. FG	M. Wieërs (Privacy & security officer)
1.1	8-3-2024	Definitieve versie	

Goedkeuring c.q. herbevestiging

Gremium	Datum
Directie en MT	31-3-2024

Voorwoord van de directie

Anno 2024 leven we in een informatiemaatschappij waarin data en informatie voor het overgrote deel uitsluitend digitaal worden uitgewisseld. Zeker na het 'Coronatijdperk' is iedereen 'online' en iedereen is tegenwoordig bekend met Big Data, datamining, desinformatie, 'fake news' en 'deep fakes', 'robotisering', algoritmen en Kunstmatige Intelligentie. Dit alles brengt nieuwe kansen met zich mee, uitdagingen, maar ook bedreigingen en soms ethische dilemma's.

Ook voor VfPf zijn data en informatie van essentiele waarde: zonder data en informatie kan VfPf niet bestaan. In dit beleidsdocument vind je daarom op hoofdlijnen een beschrijving hoe we bij VfPf omgaan met de beveiliging van data en informatie (Security). De bescherming van persoonsgegevens (Privacy) valt daar ook onder. We korten dit af tot Privacy&Security-beleid (P&S-beleid).

Het P&S-beleid draagt bij aan de continuiteit van de belangrijke opdracht die we gezamenlijk voelen: het primair onderwijs ontzorgen en ondersteunen bij het borgen van de kwaliteit en continuïteit van het onderwijs zodat lesgeven centraal kan staan. We willen kwalitatief hoogwaardige dienstverlening bieden en besluiten nemen die bijdragen aan het realiseren van onze organisatiebrede doelstellingen en de (bij)sturing daarop. In de toekomst willen we ons ontwikkelen tot een toonaangevend sectorbreed service- en kenniscentrum. Het P&S-beleid levert een bijdrage aan de kwaliteit van data en informatie waar we mee werken en draagt zo bij aan onze missie en visie. Daarnaast is er ook de juridische verplichting om persoonsgegevens te beschermen. Ik doel dan op de Algemene verordening gegevensbescherming.

Niemand zal ontkennen dat hierbij van cruciaal belang is, dat de data waarmee we werken *betrouwbaar* is. En dan rijst onmiddellijk de vraag: wanneer is data betrouwbaar? Welke kwalitatieve eisen stellen wij als VfPf eigenlijk aan onze data? En om welke soorten data gaat het dan? Aan welke bedreigingen worden die data feitelijk blootgesteld? En hoe groot is het risico dat die data daar ook door wordt getrofffen?

In deze digitaal gedomineerde samenleving onttrekt data zich aan onze fysieke waarneming en dat maakt het nu juist zo lastig, omdat op het eerste oog niet meteen zichtbaar is wat er met die data gebeurt. En juist daar gaat het om: alléén als we weten wat er precies met 'onze' data gebeurt en waardoor die data bedreigd worden, kunnen we de verantwoordelijkheid daarover nemen en de betrouwbaarheid van onze data garanderen.

Alle vragen die ik hierboven heb opgeworpen moeten we dus met elkaar beantwoorden om te komen tot een doeltreffend pakket aan maatregelen om de betrouwbaarheid van onze data te waarborgen. We doen dan wat nodig is om onze belangrijkste data sterk te beveiligen, en onze minder belangrijke data minder sterk te beveiligen. Anders gezegd: we treffen *passende* maatregelen. En steeds bekijken we, of die maatregelen nog voldoen.

Ik wijs tot slot met nadruk op de concepten *Privacy by Design and Default* en *Security by Design and Default*. Er verandert veel bij VfPf, ook de komende jaren nog. Privacy & Security moet al vanaf het begin van de ontwikkeling van nieuwe diensten en producten voor onze klanten meegenomen worden. Dit niet alleen omdat de AVG ons dat oplegt, maar vooral omdat onze klanten en stakeholders dat van ons mogen verwachten.

Denis Vijgen,

1 Doelgroep, definitie en doelstellingen P&S-beleid

1.1 Doelgroep P&S

Dit Privacy- en Securitybeleid is geschreven voor iedereen die voor VfPf werkt. Of je nu in vaste dienst bent of op tijdelijke basis voor VfPf werkt, of werkzaam bent bij één van onze leveranciers: bij VfPf moet iedereen een steentje bijdragen aan Privacy en Security. Privacy & Security raakt álle afdelingen en lagen van VfPf en álle disciplines daarbinnen. Dan kun je denken aan Directie en Management, Informatievoorziening, Informatie- en Communicatietechnologie (ICT), Personeel & Organisatie (PO), Procesmanagement, Control, Risicomanagement en Commmunicatie. Wat we in eerdere beleidsversies hebben benoemd, geldt nog steeds: Privacy & Security is van iedereen en hoort bij ons gewone, dagelijkse werk.

1.2 Definitie P&S

VfPf gebruikt bij het uitvoeren van de (wettelijke) taken allerlei gegevens, waaronder ook persoonsgegevens. Persoonsgegevens zijn gegevens die ofwel direct over iemand gaan, ofwel (zonder al te veel moeite) naar een unieke persoon te herleiden zijn. Persoonsgegevens moeten worden beschermd en dé wet die hierop toeziet is de Algemene verordening gegevensbescherming (AVG). Met de term 'Privacy' doelen we op de bescherming en beveiliging van de persoonsgegevens die VfPf gebruikt.

VfPf gebruikt naast persoonsgegevens ook andere informatie en dit wordt ook beschermd en beveiligd. Denk aan bedrijfsgevoelige informatie, zoals Jaarplannen en financiele gegevens, en aan technische data, zoals broncodes. Of denk aan informatie, die minder bedrijfsgevoelig is, zoals beleidsdocumenten, procesbeschrijvingen en werkinstructies. Denk ook aan algemene en openbare informatie over onze activiteiten, producten en diensten.

Met de term 'Security' doelen we op de beveilging van álle soorten van informatie die VfPf gebruikt. Data/informatie in de systemen en applicaties van VfPf moet betrouwbaar zijn. We drukken de betrouwbaarheid van data/informatie uit in de mate waarin die Beschikbaar, Integer en Vertrouwelijk (BIV) is.

- *Beschikbaarheid: data/informatie en systemen/applicaties moeten op de juiste momenten **Beschikbaar** zijn: hebben gebruikers op de juiste momenten toegang tot de data/informatie en systemen/applicaties die ze voor hun werk nodig hebben?*
- *Integriteit: de data/informatie en systemen/applicaties moeten **Integer** zijn: is waar we mee werken en hoe we dat doen juist, is het volledig?*
- *Vertrouwelijkheid: de data/informatie en systemen/applicaties moeten **Vertrouwelijk** zijn en blijven waar dat nodig is: hebben alléén personen toegang tot data/informatie*

1.3 Doelstellingen P&S-beleid

Dit beleid geeft de strategische richting voor het bereiken van de doelstellingen voor de bescherming en beveiliging van data/informatie. De AVG en ISO27001 (incl. ISO27002) zijn hierin leidend.

De beleidsstukken die met dit beleid samenhangen geven hier verder tactisch en operationeel invulling aan. Vooral de beleidstukken 'Classificatiebeleid', 'Technisch securitybeleid' en 'Handboek P&S' zijn daarbij van belang: deze documenten geven nadere invulling, verdieping en concretisering aan het Privacy & Securitybeleid. Gedragsregels voortvloeiend uit dit beleid zijn opgenomen in het Personeelshandboek van VfPf.

Doelstelling	Hoe te behalen
VfPf is op zo'n manier georganiseerd dat we onze werkzaamheden om het Information Security and Privacy Managementsysteem (ISPMS) in stand te houden nu én in de toekomst kunnen blijven uitvoeren conform de vereisten van het ISPMS (hierbij inbegrepen toekomstige structuurwijzigingen rondom de ISO27001 en ISO27002).	• We beleggen onze taken en verantwoordelijkheden binnen de organisatie en leggen werkwijzen en maatregelen vast (Handboek P&S, Personeelshandboek, Technisch securitybeleid etc.). • We treffen organisatorische maatregelen en leggen bewijs vast in Outlook, OneDrive, Shaprepoint of ander documentatiesysteem. •
VfPf beheerst zijn risico's op het gebied van Privacy & Security door middel van de BIV-principes.	• We voeren minimaal jaarlijks risicoanalyses uit ten aanzien van Security en leggen bewijs vast in Outlook, OneDrive, Sharepoint of ander documentatie-systeem. • We treffen technische maatregelen (reductie van kwetsbaarheden, misbruik van gegevens etc.) o.b.v. interne processen zoals de procedure BIV-classificatie en leggen bewijs vast in Outlook, OneDrive, Shaprepoint of ander documentatie-systeem.
VfPf voldoet aan beleidsregels, processen en procedures inclusief andere werkafspraken ten aanzien van Privacy & Security	• Wij trainen onze medewerkers minimaal jaarlijks op het gebied van bewustzijn en leggen bewijs vast in Outlook, OneDrive, Sharepoint of ander documentatie-systeem. • Nieuwe medewerkers krijgen binnen een maand na indiensttreding een passende bewustzijnstraining en we leggen bewijs vast in Outlook, OneDrive, Sharepoint of ander documentatie-systeem. • Jaarlijks worden interne audits uitgevoerd om te bepalen of er aan de door de organisatie gestelde eisen wordt voldaan. • Afwijkingen worden vastgelegd en vormen de basis voor continue verbetering. • Team P&S is betrokken (expliciet en impliciet) bij interne processen zoals PPMO, P&D, Change en het Inkoopproces. • Team P&S monitort ontwikkelingen en veranderingen op gebied van wet- en regelgeving en heeft contacten met Overheidsorganisaties op dit punt.

2 AVG en ISO27001

Bij VfPf wordt Privacy en Security (lees: de veilige en zorgvuldig omgang met data/informatie en systemen/applicaties) vormgegeven door twee belangrijke kaders, te weten:

- AVG (incl. de Uitvoeringswet AVG)
- ISO 27001 en ISO27002

Zowel op grond van de AVG als op grond van de ISO 27001 en ISO27002 moet VfPf "*passende technische en organisatorische maatregelen*" treffen om (persoons-)gegevens en data/informatie te beveiligen. VfPf realiseert dit door middel van interne beleid/procedures/processen op het gebied van dataclassificatie en risicoanalyses.

Dataclassificering en risicoanalyses geven antwoord op de vraag welke technische en organisatorische maatregelen moeten worden getroffen om ervoor te zorgen dat de data/informatie de juiste mate van Beschikbaarheid, Integriteit en Vertrouwelijkheid bezit en tevens blijft bezitten.

2.1 Passende technische & organisatorische maatregelen

Dataclassificatie begint bij het aanmaken van Informatiegroepen. Dat zijn soorten informatie die een bepaalde mate van vertrouwelijkheid gemeen hebben. Bij VfPf onderscheiden we openbare, interne, bedrijfsvertrouwelijke en vertrouwelijke informatie. Deze 4 Informatiegroepen zijn omschreven in onderstaande tabel. De blauwe kolom maakt in één oogopslag duidelijk hoe vertrouwelijk we die data/informatie vinden en aan wie we die data/informatie dus kunnen/mogen verstrekken.

Omschrijving Informatiegroep	Wettelijke eisen	Classificatie Vertrouwelijkheid
Algemene en publiekelijk beschikbare informatie over activiteiten, producten en diensten van VfPf, zoals folders, leaflets, flyers, presentaties, rapportages en onderzoeken, bestuursbesluiten op de website VfPf, etc.	Geen	**Openbaar:** Informatie is publiekelijk beschikbaar en mag vrijelijk verstrekt worden
Operationeel beleid, processen, procedures, plannen, rollen etc.	Geen	**Intern gebruik:** Informatie is beschikbaar voor alle interne medewerkers en door het management geselecteerde derde partijen. Deze informatie mag uitsluitend aan interne medewerkers en door het management geselecteerde derde partijen verstrekt worden
(Commercieel) vertrouwelijke stukken, zoals offertes, prijsopgaves, contracten, facturen en andere documenten met commercieel vertrouwelijke informatie. Verder bedrijfsinformatie over derde partijen (kengetallen, solvabiliteit e.d.) waarover VfPf beschikt, bv. in het kader van due diligence, etc. Verder ook de uitkomsten/rapportages over bv. penstesten in het kader van P&S, technische gegevens, configuraties, broncode, etc.	Wet toezicht financiële verslaglegging (Wtfv), Aanbestedingswet 2012	**Bedrijfsvertrouwelijk**: Informatie is uitsluitend en exclusief beschikbaar voor geautoriseerde personen. De informatie mag alleen aan deze geautoriseerde personen worden verstrekt, niet aan derde partijen (tenzij hiertoe noodzaak bestaat en er zwaarwegende redenen zijn)
Persoonsgegevens van klanten, consumenten, werknemers en Bestuursleden, AC-leden etc.	Algemene verordening gegevensbescherming (AVG), Uitvoeringswet AVG (UAVG) en Telecommunicatiewet	**Persoonsgegevens**: Persoonsgegevens (waaronder bijzondere) – als bedoeld in art. 4 lid 1 AVG) zijn uitsluitend beschikbaar voor geautoriseerde personen. De informatie mag alleen aan geautoriseerde personen verstrekt worden, niet aan derde partijen (tenzij hiertoe noodzaak bestaat en er zwaarwegende reden zijn)

Het Technisch securitybeleid van VfPf beschrijft de basisset aan maatregelen die gelden voor deze data/informatie in onze systemen/applicaties.

Als de BIV-classificatie van data/informatie in (de context van) onze systemen/applicaties een hogere BIV-score oplevert, stappen we over naar een scherpere en aanvullende set met technische maatregelen. Deze maatregelen zijn opgenomen in de Maatregelenmatrix.

Zo kunnen we een hoger beschermingsniveau garanderen. Afhankelijk van specifieke risico's die we in risico-analyses zien en afhankelijk van de context waarbinnen de maatregelen bepaald worden, passen we de totale set technische en organisatorische maatregelen indien nodig nóg verder aan.

2.2 De AVG toegelicht

De AVG beschijft niet concreet wat wél en wat niet mag met persoonsgegevens, maar geeft een aantal beginselen bij het gebruik ervan. Deze beginselen zijn vast onderdeel van de processen van VfPf waarin P&S een 'haakje' heeft zoals het PPMO/P&D-proces, Inkoopproces, (pre)DPIA-proces en Changeproces. Team P&S beantwoordt vraagstukken in relatie tot deze beginselen vanuit de context van de organisatie en daaronder hangende (sub)afdelingen en processen. In een notendop kunnen die beginselen als volgt worden samengevat:

- *VfPf maakt alleen gebruik van persoonsgegevens als daar een juridische basis voor is. In de AVG heet dat **Gerechtvaardigde grondslag**. Als we gebruik maken van persoonsgegevens zorgen we ervoor dat de personen over wie het gaat over dat gebruik zijn ingelicht. Dit doen we door een zogenaamde **Privacyverklaring** op te stellen en te publiceren. Zo'n verklaring wordt ook wel het Privacy Statement genoemd. Het spreekt voor zich dat een Privacyverklaring actueel moet worden gehouden.*
- *Als VfPf gebruik maakt van persoonsgegevens zorgen we ervoor dat we hebben beschreven waarom/waarvoor we die persoonsgegevens gebruiken (het zogenaamde "doeleinde"). Willen we die persoonsgegevens voor een ánder doel gaan gebruiken, dan is dat alleen toegestaan als dat andere doel inhoudelijk samenhangt met het doel waarvoor de gegevens aanvankelijk werden gebruikt. In de AVG heet dat **Doelbinding ("niet onverenigbare verdere verwerking").***
- *VfPf maakt alléén gebruik van persoonsgegevens die werkelijk nodig zijn voor de uitvoering van ons werk. In de AVG heet dit **Minimale gegevensverwerking.***
- *VfPf maakt gebruik van persoonsgegevens die juist zijn en we actualiseren die persoonsgegevens.*
- *VfPf bewaart persoonsgegevens niet langer dan nodig is. Daarom leggen we de Bewaartermijn van persoonsgegevens vast en verwijderen we die persoonsgegevens als die termijn voorbij is.*
- *VfPf neemt "**passende technische en organisatorische maatregelen**" om de persoonsgegevens die we gebruiken te beveiligen. Dit betekent dat we kiezen voor een niveau van beveiliging dat past bij de **risico's** die we daarbij inschatten.*

Verder brengt de AVG een aantal concrete verplichtigen voor VfPf met zich mee. In een notendop kunnen die verplichtingen als volgt worden samengevat:

- *VfPf moet "passende technische en organisatorische maatregelen" nemen om ervoor te zorgen dat de AVG wordt toegepast.*
- *VfPf past Privacy by Design toe, vertaald als gegevensbescherming door ontwerp. Dit betekent dat we bijvoorbeeld al bij de aanbesteding van een opdracht rekening houden met eisen op het gebied van P&S. Het betekent bijvoorbeeld ook dat we bij het bouwen van een applicatie al nadenken over eisen op het gebied van P&S. Ook past VfPf Privacy by Default toe, vertaald als gegevensbescherming door standaardinstellingen. Dit betekent dat we al aan de start van innovaties en/of verbeteringen Privacy & Security-beginselen toepassen, en niet pas achteraf.*
- *Als VfPf samen met een andere organisatie persoonsgegevens gebruikt, spreken we af welke organisatie welke verantwoordelijkheden draagt.*
- *VfPf mag een derde partij opdracht geven de werkzaamheden met persoonsgegevens uit te voeren (uitbesteden). Zo'n partij heet in de AVG: Verwerker. Voorwaarde hiervoor is dat we met Verwerkers een Verwerkersovereenkomst sluiten. De AVG bevat een aantal eisen waar zo'n Verwerkersovereenkomst aan moet voldoen.*
- *Vfpf houdt een Verwerkingsregister bij. In dat register nemen we per Verwerking van persoonsgegevens minstens de door de AVG voorgeschreven gegevens op.*
- *VfPf meldt binnen 72 uur na ontdekking van een datalek dat datalek bij de Autoriteit Persoonsgegevens. Als dit datalek een hoog risico voor betrokkenen inhoudt meldt VfPf dat ook bij die betrokkenen. Zo stellen we betrokkenen in staat om zelf eventuele risico's aan te pakken.*
- *VfPf voert een risico-analyse uit bij gebruik van persoonsgegevens dat waarschijnlijk een hoog risico voor betrokkenen oplevert. In de AVG heet dit een Data Protection Impact Assessment.*
- *VfPf stelt een Functionaris voor Gegevensbescherming aan (afgekort tot FG). De belangrijkste taak van de FG is toezien op de naleving van de AVG en het P&S-beleid van VfPf.*

2.3 De ISO27001 (incl. ISO27002) toegelicht

De ISO27001 beschrijft in feite de voorwaarden waaraan een zogenaamd Information Security Management System (ISMS) moet voldoen. VfPf heeft dit beschreven in het 'Handboek P&S'.

Het ISMS is bij VfPf de motor van de activiteiten op het gebied van P&S en wordt onderhouden middels de plan-do-check-act cyclus. Het doel van een ISMS is continu beoordelen of de beveiligingsmaatregelen – die voortvloeien uit de ISO27002 - passend en effectief zijn, en of deze bijgesteld moeten worden. Een belangrijk uitgangspunt is hierbij dat we denken in termen van risico's en die risico's prioriteren. Daarom brengen we in die risico's een rangorde aan: Hoog, Midden of Laag. Uitgangspunten bij de omgang met deze risico's zijn:

- *Als een risico als 'laag' wordt bestempeld dan kiezen we ervoor om dat risico te accepteren, tenzij het niet aanpakken van een laag risico op termijn tot een hoger risico kan leiden.*
- *Als een risico als 'midden' of 'hoog' wordt bestempeld neemt de risico-eigenaar in overleg met de directie altijd maatregelen, tenzij dat niet mogelijk is en/of de baten niet opwegen tegen de kosten.*

3 Verantwoordelijkheden P&S

3.1 Algemene verantwoordelijkheid medewerkers

VfPf verwacht van mensen die voor VfPf werkzaam zijn, dat ze zich bewust zijn van de risico's die er zijn als het gaat om data/informatie. Veilig werken met data/informatie in onze systemen is een verplicht onderdeel van ieders takenpakket.

Om te helpen bij het vergroten van het risicobewustzijn biedt VfPf met geregelde tussenpozen awareness-sessies en trainingen aan op het gebied van P&S. Zo bereiken we dat iedereen zich bewust is van risico's op het gebied van P&S en in staat is veilig om te gaan met data/informatie. Ín het uiterste geval kunnen zelfs disciplinaire maatregelen worden genomen. Dit is voor interne medewerkers vastgelegd in het Personeelshandboek dat onlosmakelijk onderdeel uitmaakt van ieders arbeidsovereenkomst met VfPf.

Als het gaat om externe medewerkers zijn verantwoordelijkheden ten aanzien van P&S vastgelegd in een overeenkomst van opdracht.

Iedereen werkzaam voor VfPf moet Security-incidenten en Datalekken kunnen herkennen en deze zo snel mogelijk per telefoon of e-mail melden bij de Security Officers van VfPf.

3.2 Naleving

Om er zeker van te zijn dat Privacy en Security bij VfPf écht werkt, worden alle beveiligingsmaatregelen gecheckt door interne - en externe controles. Met controles kunnen we aantonen, ook aan derden, dat het P&S-beleid gevolgd wordt. Dit betekent onder andere dat:

- *We controleren dat werknemers veilig werken, als onderdeel van het werk;*
- *We periodiek interne en externe controles en audits uitvoeren om het beleid te controleren;*
- *We actie nemen als uit controles en audits afwijkingen naar voren komen.*

4 Slotopmerkingen

De Directie wordt over dit P&S-beleid - en alle daaruitvoortvloeiende werkzaamheden - geadviseerd door Team P&S. De Directie stelt het P&S-beleid vast.

Het management van VfPf is eindverantwoordelijk voor de uitvoering van het P&S-beleid. Team P&S monitort de naleving van het beleid en adviseert de Directie over handhaving. Eens per drie jaar herzien we ons P&S-beleid, of zoveel eerder als daar concreet aanleiding voor is.

De Functionaris voor de Gegegevensbescherming is hierbij op grond van de AVG een onafhankelijke toezichthouder die erop toeziet dat VfPf conform de AVG handelt. Verder is de FG contactpersoon in de samenwerking en contacten tussen de Autoriteit Persoonsgegevens (AP) en het VfPf.

5 Referentiedocumenten

- Algemene verordening gegevensbescherming (AVG);
- ISO27001 (incl. ISO27002);
- Handboek P&S VfPf;
- Classificatiebeleid VfPf;
- Technisch beleid VfPf;
- Personeelshandboek;
- Incident response plan.